WE CLAIM:

1. A compact dual function Random Number Generator (RNG) and Stream Cipher Generator (SCG) including a Crypto-engine and a controller for controlling the Crypto-engine to operate either as a RNG or a SCG, including three muliplexers controlled by the controller to supply signals selectively to and receive signals from the Crypto-engine, in which a first multiplexer is arranged to receive RNG seed signals or SCG key signals, a second multiplexer is arranged to receive dynamic synchronization parameter signals or constant synchronization signals, and a third multiplexer is arranged to receive signals from the Crypto-engine and provide Random Number output signals or Stream Cipher output signals, respectively in each case.

2. A compact dual function Random Number Generator (RNG) and Stream Cipher Generator (SCG) according to claim 1, including an XOR gate arranged to receive the Stream Cipher output signals from the third multiplexer and separate Stream Cipher signals in plaintext or ciphertext, such that the output of the XOR gate is in ciphertext or plaintext, respectively.

3. A compact dual function Random Number Generator (RNG) and Stream Cipher Generator (SCG) according to claim 1, including a plurality of clipped Hopfield

Neural Network pairs.

4. A compact dual function Random Number Generator (RNG) and Stream Cipher Generator (SCG) according to claim 3, including a Seed/Key input; a Synchronization Parameter Input; a Seed/Key Randomizer and a Non-Linear Manipulator.

5. A compact dual function Random Number Generator (RNG) and Stream Cipher Generator (SCG) according to claim 4, in which the clipped Hopfield Neural Network pairs in which an Input CHNN (ICHNN) provides a nonlinear interaction with a dynamic/constant Synchronization Parameter input and an output CHNN (OCHNN) provides nonlinear interaction with an adjacent ICHNN output.

6. A compact dual function Random Number Generator (RNG) and Stream Cipher Generator (SCG) according to claim 3, including one of a single iterating CHNN pair and a k pipeline CHNN pair, a Decision Box (DEC) and an Attractor Mapping Table (AMT).

7. A compact dual function Random Number Generator (RNG) and Stream Cipher Generator (SCG) according to claim 3, including neurons in two states {0,1}; Synaptic Weights in three states {-1,0,1}; and a non-linear Activation Function {0,1}.

8. A compact dual function Random Number Generator (RNG) and Stream Cipher Generator (SCG) according to claim 3, in which an input to a n-neuron Clipped Hopfield Neural Network pair is arranged to converge to one of the 2n+1 stable states or attractors of the network after finite steps of iterations k.

9. A compact dual function Random Number Generator (RNG) and Stream Cipher Generator (SCG) according to claim 3, in which the clipped Hopfield Neural Network is constructed using cascaded Lookup Tables if n is small.

10. A compact dual function Random Number Generator (RNG) and Stream Cipher Generator (SCG) according to claim 9, in which the Lookup Tables are associated with an initial Synaptic Weight Matrix and a random selected Permutated Synaptic Weight Matrix in other instants.

11. A compact dual function Random Number Generator (RNG) and Stream Cipher Generator (SCG) according to claim 3, including a "toggle" feature in some selected bit sequence combination to avoid statistical bias and possible correlation attack.